IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Massimiliano Antonio Poletto et al.	Art Unit	: 2134
Serial No.	: 10/066,252	Examiner	: Nalven Andrew, I
Filed	: January 31, 2002	Conf. No.	: 2792
Title	: ARCHITECTURE TO THWART DENIAL OF SERVICE ATTACKS		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF ON BEHALF OF MASSIMILIANO ANTONIO POLETTO ET AL. (CORRECTED)

The Appeal Brief fee has previously been paid. If any additional charges or credits are due, please to Deposit Account No. 06-1050.

(i.) Real Party In Interest

The real party in interest in the above application is Mazu Networks, Inc.

(ii.) Related Appeals and Interferences

The appellant is not aware of any appeals or interferences related to the above-identified patent application.

(iii.) Status of Claims

This is an appeal from the decision of the Primary Examiner in an Office Action dated May 12, 2006, rejecting claims 1-25 and 27-34, all of the claims in the application. There was not a claim 26 originally filed. Claims 1-25 and 27-34 are the subject of this appeal.

(iv.) Status of Amendments

Appellant filed a Reply to the Office Action dated May 12, 2006 to the status of claim 20 as "original." Appellant also amended claims 1 and 11 to correct the informalities pointed out by the examiner and corrected minor informalities in claim 3. Appellant also attempted to renumbered claims 27-34 as claims 26-33.

In an advisory action dated September 6, 2006, the examiner did not enter the attempted re-numbering of claims 27-34 electing instead to defer re-numbering by examiner's amendment upon allowance. Otherwise, the examiner indicated entry of the amendment. Accordingly, all substantive amendments have been entered. Appellant filed a Notice of Appeal on August 14, 2006, which was received by the Office on August 17, 2006.

(v.) Summary of Claimed Subject Matter

Claim 1

One aspect of Appellant's invention is set out in claim 1 as a monitoring device disposed for thwarting denial of service attacks on a data center. "Referring to FIG. 1, an arrangement 10 to thwart denial of service attacks (DoS attacks) is shown." [Appellant's specification Page 4, lines 22-23]. "Some or all of the deployed monitor devices in the arrangement are provisioned monitors." [Appellant's specification Page 5, lines 29-30].

Inventive features of claim 1 include a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links "Referring now to FIG. 2, the data center 20 has a plurality of links 21a-21n with the Internet 14. Each customer Ci (0 <= i < N, for N customers) of the data center is associated with a set of addresses Ai. The provisioned monitor has a notion of inbound and outbound packets, obtained directly from the physical link's transmit and receive ports." [Appellant's specification Page 7, lines 6-11]. and collect statistical information on packets that are sent between the network and the data center over the coupled physical links for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to. "Probes 26a-26n perform several functions such as sampling of packets and collect information pertaining to statistical properties of the packets." [Appellant's specification Page 8, lines 10-13]. "A service provider that provides a provisioned monitor 26 could perform ingress filtering on traffic entering its network from customers downstream of the provisioned monitor. In this way, any outbound packets with unknown source addresses (not in any address of address space Ai) are considered to be originating from unprovisioned customers rather than being part of a spoofed DoS attack." [Appellant's specification Page 7, lines 22-28].

Claim 7

Claim 7 claims another aspect of the invention. Claim 7 is directed to a method of thwarting denial of service attacks on a victim data center coupled to a network. This feature is supported by the analogous feature of claim 1 and FIG. 7B.

Inventive features of claim 7 include collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on. This feature is supported as the analogous feature of claim 1.

Inventive features of claim 7 also include communicating data, over a dedicated network, to a control center. This feature is supported as the analogous feature of claim 1 and "In some embodiments, the control center 24 is coupled to the gateways 26 and data collectors 28 by a

hardened, redundant network 30. In preferred embodiments, the network is inaccessible to the attacker. [Appellant's specification Page 5, lines 16-20].

Claim 11

Another aspect of the invention is covered by claim 11. Claim 11 is directed to an arrangement to monitor a link between a data center and a network for thwarting denial of service attacks on the data center. This feature is supported by the analogous feature of claim 1.

Inventive features of claim 11 include, a provisioned monitor, placed on selected links in the data center so that the provisioned monitor examines traffic entering or leaving that data center on the selected links and collects statistical information for a plurality of provisioned customers, which are on links that are downstream from the selected links that the provisioned monitor is disposed on, This feature is supported by the analogous feature of claim 1. The provisioned monitor maintaining separate counter logs for each provisioned customer. "Each provisioned monitor keeps separate counter logs 52a-52d for each provisioned customer (virtual monitor)." [Appellant's specification Page 11, lines 29-31].

Inventive features of claim 11 also include a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to. "... as well as a global counter log 52 that accounts for all traffic seen on the link." [Appellant's specification Page 11, lines 31-32].

Claim 24

Claim 24 is directed a method of thwarting attacks on a victim data center coupled to a network. This feature is supported by the analogous feature of claim 1 and FIG. 7B.

Inventive features of claim 24 include collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs. "Referring now to FIG. 2, the data center 20 has a plurality of links 21a-21n with the Internet 14. Each customer Ci ($0 <= i < N$, for N customers) of the data center is associated with a set of addresses Ai. The provisioned monitor has a notion of inbound and outbound packets, obtained directly from the physical link's transmit and receive ports." [Appellant's specification Page 7, lines 6-11].

Inventive features of claim 24 include maintaining separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the links on which collecting occurs. This feature is supported as the analogous feature of claim 11. "Each provisioned monitor keeps separate counter logs 52a-52d for each provisioned customer (virtual monitor)." [Appellant's specification Page 11, lines 29-31] "... as well as a global counter log 52 that accounts for all traffic seen on the link." [Appellant's specification Page 11, lines 31-32].

Claim 29

Claim 29 is directed to a method of thwarting attacks on a victim data center coupled to a network. This feature is supported as the analogous feature of claim 1.

Inventive features of claim 29 include collecting statistical information for a plurality of links that are downstream from links on which collecting occurs. This feature is supported as the analogous feature of claim 1

Inventive features of claim 29 include performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic. "Packet analysis for a particular virtual monitor happens by classifying packets based on addresses at the time of the analysis." [Appellant's specification Page 12, lines 3-5].

Inventive features of claim 29 also include communicating alerts that arise from the traffic analysis. "The method also includes communicating alerts that arise from the traffic analysis." [Appellant's specification Page 2, line 31 to page 3, line 2].

(vi.) Ground of Rejection to be Reviewed on Appeal

Claims 1-25 and 27-34 stand rejected under 35 U.S.C. 102(e) as being anticipated by Ioele et al US Patent No. 7,007,299.

(vii.) Argument

Anticipation

"It is well settled that anticipation under 35 U.S.C. §102 requires the presence in a single reference of all of the elements of a claimed invention." *Ex parte Chopra*, 229 U.S.P.Q. 230, 231 (BPAI 1985) and cases cited.

"Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

"This court has repeatedly stated that the defense of lack of novelty (i.e., 'anticipation') can only be established by a single prior art reference which discloses each and every element of the claimed invention." *Structural Rubber Prod. Co. v. Park Rubber Co.*, 223 U.S.P.Q. 1264, 1270 (Fed. Cir. 1984), citing five prior Federal Circuit decisions since 1983 including *Connell*.

In a later analogous case the Court of Appeals for the Federal Circuit again applied this rule in reversing a denial of a motion for judgment n.o.v. after a jury finding that claims were anticipated. *Jamesbury Corp. v. Litton Industrial Prod., Inc.*, 225 U.S.P.Q. 253 (Fed. Cir. 1985).

After quoting from *Connell*, "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim," 225 U.S.P.Q. at 256, the court observed that the patentee accomplished a constant tight contact in a ball valve by a lip on the seal or ring which interferes with the placement of the ball. The lip protruded into the area where the ball will be placed and was thus deflected after the ball was assembled into the valve. Because of this constant pressure, the patented valve was described as providing a particularly good seal when regulating a low pressure stream. The court quoted with approval from a 1967 Court of Claims decision adopting the opinion of then Commissioner and later Judge Donald E. Lane:

> [T]he term "engaging the ball" recited in claims 7 and 8 means that the lip contacts the ball with sufficient force to provide a fluid tight seal **** The Saunders flange or lip only sealingly engages the ball 1 on the upstream side when the fluid pressure forces the lip against the ball and never sealingly engages the ball on the downstream side because there is no fluid pressure there to force the lip against the ball. The Saunders sealing ring provides a compression type of seal which depends upon the ball pressing into the material of the ring. *** The seal of Saunders depends primarily on the contact between the ball and the body of the sealing ring, and the flange or lip sealingly contacts the ball on the upstream side when the fluid pressure increases. 225 U.S.P.Q. at 258.

Relying on *Jamesbury*, the ITC said, "Anticipation requires looking at a reference, and comparing the disclosure of the reference with the claims of the patent in suit. A claimed device is anticipated if a single prior art reference discloses all the elements of the claimed invention as arranged in the claim." *In re Certain Floppy Disk Drives and Components Thereof*, 227 U.S.P.Q. 982, 985 (U.S. ITC 1985).

Claims 1-25 and 27-34 are not anticipated by Ioele et al US Patent No. 7,007,299.

Claims 1 and 5

For the purposes of this appeal only, claims 1 and 5 stand or fall together. Claim 1 is representative of this group of claims.

Claim 1 is directed to a monitoring device disposed for thwarting denial of service attacks on a data center. Claim 1 includes the feature of a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links and collect statistical information on packets that are sent between the network and the data center over the coupled physical links for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

The examiner contends that:

> **With regards to claim 1, Ioele teaches a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links (Ioele, Figure 1, column 3 lines 25-35, column 4 lines 35-37) and collect statistical information on packets that are sent between a network and the data center for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is on (Ioele, column 6 lines 31-46).**

Appellant disagrees. Ioele fails to describe or suggest a device placed on selected links in the data center ... that collects statistical information on packets that are sent between a network and the data center for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to. Rather, Ioele discloses:

> **For example, the size of the Internet connections can be at 100 Mbps. FIG. 1 depicts the network security measures for an Internet hosting site 100. The first level of this security comprises routers 110, such as a pair of CISCO 7200 Routers, that limit external access to the network by the type of Internet traffic. The second level of security is maintained by a plurality of firewalls 121 and 122, such as Cyberguard Firewalls, with one as primary and the other as backup. The firewalls 121 and 122 communicate with each other via an interconnection 160, such as an Ethernet or fiber-optic connection. (Ioele Col. 3, lines 25-35)**
>
> **Any user requests coming from the Internet to any of the hosted sites must first go through this aggregated bandwidth to a main set of network routers 110, which functions as the first level of network security. The routers 110 screen the requests to limit external access to the network of hosted sites by the type of Internet traffic. (Ioele Col. 4, lines 35-37).**

Ioele describes a system and method for providing security to Internet hosting sites. However, nowhere does Ioele disclose a device... disposed to examine traffic entering or leaving that data center on the coupled physical links. In particular, Ioele does not disclose any device that collects statistical information on packets sent between the network and the data center ..., much less a device that collects statistical information on packets, or a device that does so for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is coupled to.

Ioele discusses network security measures for an Internet hosting site 100 at Col. 3, line 37: "The first level of this security this security comprises routers 110 ... that limit external access to the network by the type of Internet traffic." Ioele also has a second level of security ... maintained by a plurality of firewalls 121 and 122 ... that communicate with each other via an interconnection 160... ." Ioele describes a hierarchical arrangement to provide security using routers and firewalls. While Ioele mentions that: "Any user requests coming from the Internet to any of the hosted sites must first go through this aggregated bandwidth to a main set of network routers 110, which functions as the first level of network security" and that: "[T]he routers 110 screen the requests to limit external access to the network of hosted sites by the type of Internet traffic." (Ioele Col. 4, lines 35-37), Ioele fails to describe or suggest a device... that collects statistical information on packets sent between the network and the data center. No mention is made in Ioele of collection of statistical information on packets. Ioele therefore inherently cannot teach that the collection of the statistical information is made by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

In the advisory action dated September 6, the examiner states:

> **... does NOT place the application in condition for allowance because: Applicant's arguments are not persuasive Applicant has argued that Ioele fails to teach "a device disposed to examine traffic entering or leaving a data center on the coupled physical links." Examiner respectfully disagrees, Ioele teaches a device disposed to examine traffic entering or leaving a data center on the couple physical links Ioele, column 3 lines 25-35, column 4 lines 35-57, column 16 lines 31-50, Figure 1) by teaching routers/firewalls/intrusion detectors disposed to examine traffic entering or leaving the data center. Statistical information is collected in that the intrusion detectors "gather different data relating to the originating points of the requests" and create event logs Applicant further argues that there is no dedicated private network between the monitoring device and the control center disclosed by Ioele. Examiner respectfully disagrees, Ioele discloses in Figure 1, a control center (Item 140) being connected to the monitoring device where the control center is behind the routers and firewalls. Thus, Ioele teaches the control center within the data center's private network.**

Appellant contends that the examiner has not fully considered all of the limitations of claim 1. Specifically the examiner does not consider that event logs and statistical information are not equivalent and that the claim requires that ... the device disposed to examine traffic entering or leaving that data center ... as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to. This feature that the device examines traffic from a downstream perspective is not suggested by any teaching in Ioele.

The Examiner point to Ioele's teachings at column 3 lines 25-35, column 4 lines 35-57, column 16 lines 31-50, and Figure 1 for teaching: "a device disposed to examine traffic entering or leaving a data center on the couple physical links by teaching routers/firewalls/intrusion detectors disposed to examine traffic entering or leaving the data center. While arguable the examiner can argue that routers/firewalls/intrusion detectors are connected to physical links, it is clear from Ioele that Ioele fails to teach that the routers/firewalls/intrusion detectors collect the claimed statistical information and particularly fail to teach to collect statistical information on packets ... for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

The examiner also argues that the statistical information corresponds to the event log teaching of Ioele. However, Ioele discusses:

> **A fourth level of security is maintained by an operations and event log management system 140 as shown in FIG. 1, which monitors for indication of software, hardware, network and security problems, and other event logs. For**

instance a Tivoli TEC engine may be used for event log management. The Tivoli TEC engine is run on its own server and is used to roll up and monitor all event logs in the Internet hosting site. This allows the NSA of the Internet hosting site to catch any security issue or other areas of concern that may arise. Tivoli ensures the continuity of event log data by constantly monitoring the size of all NT event logs. When a log reaches a user-defined threshold, it is transferred to a central management system using a secure store and forward mechanism.

Neither Ioele nor the examiner however explains how the event logs taught by Ioele correspond to the claimed statistical information. Also, the examiner fails to explain what the relevance to claim 1 is by Ioele teaching that: "When a log reaches a user-defined threshold, it is transferred to a central management system using a secure store and forward mechanism." A secure store and forward mechanism merely relates to how the files are sent for storage. Clearly, this statement by the examiner has absolutely no relevance to any feature of claim 1.

In addition, Ioele has in the second level of network security, intrusion detectors 131, 132 located before and after the firewalls 121, 122. The intrusion detectors monitor network traffic for attack signatures. Attack signatures are discussed by Ioele as: "These engines run on a dedicated host and monitor network traffic for attack signatures and alert personnel when an attack is detected. The engine 351/352 looks for a select combination of packets that matches any profile of comprehensive list of well-known attacks." [Ioele, Col. 9, Lines 61-66]. Attack signatures are not the claimed statistical information.

Appellant contends that neither Ioele's event logs nor attack signatures are the claimed statistical information. Appellant further contends that Ioele does not suggest the claimed mechanism to protect provisioned customers sites from attack, but instead proposes that: "The Internet connections to each site are also sufficiently large to prevent flooding attacks. According to an embodiment of the present invention, the size of the Internet connections is based on the load, i.e., the number of users that will be connected to each site at once, with the size based on ten to fifty times the actual or estimated load." [Ioele Col. 3, lines 19-21]. While this may protect connections from a denial of service attack, applicant's claim 1, is directed to protecting the data center from attacks. The mechanism employed by Ioele (namely sufficiently large connections, redeployment of a web site and IDS systems as mentioned by Ioele) is substantially different than the claimed arrangement involving a device to examine traffic

entering or leaving the data center on the coupled physical links and to collect statistical information on packets.

Accordingly, since Ioele fails to describe all of the features of claim 1 arranged as in the claim, Ioele cannot anticipate claim 1.

Claim 2

Claim 2 further limits claim 1, and recites that: "the monitoring device is coupled to a control center through a dedicated, private network. This feature is not described by Ioele.

In the advisory action, the examiner argues that:

> **Applicant further argues that there is no dedicated private network between the monitoring device and the control center disclosed by Ioele. Examiner respectfully disagrees. Ioele discloses in Figure 1, a control center (Item 140) being connected to the monitoring device where the control center is behind the routers and firewalls. Thus, Ioele teaches the control center within the data center's private network.**

The examiner readily admits that the control center item 40 is behind the routers and firewalls, and thus the examiner argues that the control center is within the data center's private network. However that is not what Appellant claims, rather Appellant claims that the there is a dedicated, private network coupling the control center and the monitoring device.

Accordingly, since Ioele fails to describe all of the features of claim 2 arranged as in the claim, Ioele cannot anticipate claim 2.

Claim 3

Claim 3 further limits claim 2, and requires that the device include a communication process that communicates the statistical information on packets with the control center, and which receives queries or instructions from the control center.

Ioele fails to mention any device that communicates statistical information on packets with the control center or which receives queries from the control center. Ioele discloses event logs not statistical information on packets.

Claim 4

Claim 4 further limits claim 1 by requiring that the monitoring device is a gateway device and that it includes a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack. Neither the router nor the firewall nor the intrusion detection system nor the event log management system 140 is a gateway device. Moreover, none of those devices mentioned by Ioele install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

Ioele discloses that: "Like the firewalls, the detectors 131, 132 also have their own set of built-in triggers and filters." However, the built-in triggers and filters do not meet the claimed element of a process to install filters .... Ioele also discloses that: "Tivoli provides configuration facilities and a browser with extensive filtering to allow ad-hoc queries and printing of centrally stored event logs and event correlation." This however has no relevance to the claimed process for install filters .... In addition, Ioele also discloses that: "The management console 353 controls the engines 351, 352 by issuing start, stop, or pause commands. It also reconfigures attack signatures, filters, and event responses as well as exchange keep alive messages." and also mentions port filtering. However, again this does not describe a process "to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack."

Claim 6

Claim 6 further limits claim 4 to require that the gateway includes "a process to aggregate traffic from the various links and to produce logs and detection heuristics." While Ioele clearly mentions logs, it is not at all clear that the event logs of Ioele result from aggregated traffic from the various links. Nevertheless, this event logs do not describe or suggest the statistical information of base claim 1 and thus, claim 6 at least serves further distinguish base claim 1 from Ioele.

Claims 7 and 9

For the purposes of this appeal only, claims 7 and 9 stand or fall together. Claim 7 is representative of this group of claims.

Claim 7 is directed to a method of thwarting denial of service attacks on a victim data center. Claim 7 includes the features of collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on and communicating data, over a dedicated network, to a control center.

The salient features of claim 7 include that collecting statistical information is performed using a provisioned monitor, namely that collection is performed on a customer basis as if the collection was being perform on links that were down stream from the links that the provisioned monitor is disposed on.

While Ioele mention re-provisioning of firewall traffic [Ioele Col. 4, line 5], Ioele does not discuss any concept of provisioning of a device for collection of statistical data on a customer basis as if the collecting was occurring on links downstream from the links that the monitor is disposed on. As discussed in claim 1, Ioele does not collect statistical information on packets sent between a network and a plurality of customers. Ioele, in contrast, uses Intrusion detection schemes that look for attack signatures. Attack signatures however are not based on collection of statistical information on packet flows but instead on known, pre-established templates of packet contents that are deemed an attack. Neither the attack signatures nor any other feature of Ioele are done on a provisioning customer basis

Claim 8

Claim 8, which recites that the device is a gateway device and further includes installing filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack, is allowable for analogous reasons to those given in claim 4

Claim 10

Claim 10 distinguishes since Ioele does not describe collecting of statistical information, as argued above, or that collecting occurs for either inbound or outbound traffic or both.

Claims 11 and 12

For the purposes of this appeal only, claims 11 and 12 stand or fall together. Claim 11 is representative of this group of claims.

Claim 11 calls an arrangement disposed to monitor a link between a data center and a network for thwarting denial of service attacks on the data center. Claim 11 includes a provisioned monitor, placed on selected links in the data center ... that ... examines traffic entering or leaving that data center ... and collects statistical information for a plurality of provisioned customers ... the provisioned monitor maintaining separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.

Claim 11 includes the features of a provisioned monitor that collects statistical information for a plurality of provisioned customers, which for reasons discussed above are not described or suggested by Ioele. In addition, claim 11 includes the feature that the provisioned monitor maintains separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.

The examiner contends with respect to these later features that Ioele teaches: "... the provisioned monitor maintaining separate counter logs for each provisioned customer (Ioele, column 6 lines 45-46) and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to (Ioele, column 7 lines 37-64)."

Ioele does not specifically suggest, much less describe either the separate counter logs for each provisioned customer or the global counter log that accounts for all traffic seen on the link. Accordingly to Ioele, at Col. 7 lines 37-64:

> **A fourth level of security is maintained by an operations and event log management system 140 as shown in FIG. 1, which monitors for indication of software, hardware, network and security problems, and other event logs. For instance a Tivoli TEC engine may be used for event log management. The Tivoli TEC engine is run on its own server and is used to roll up and monitor all event logs in the Internet hosting site. This allows the NSA of the Internet hosting site to catch any security issue or other areas of concern that may arise. Tivoli ensures the continuity of event log data by constantly monitoring the size of all NT event logs. When a log reaches a user-defined threshold, it is transferred to a central management system using a secure store and forward mechanism. Tivoli provides configuration facilities and a browser with extensive filtering to allow ad-hoc queries and printing of centrally stored event logs and event correlation. A script will run to extract pertinent information from the logs using Tivoli. This script will**

be developed by an Operations Manager of the Internet hosting site to provide the ISA with information. The script and the information it provides may be reviewed by appropriate host personnel to ensure that the ISA will have the data necessary to oversee the security of the system. All data from these logs is to be stored for a predetermined period of time. The NSA monitors the TEC and takes appropriate actions for all security related alarms. The NSA and ISA have read access to the event log management server. Again, the ISA approves access to this server.

Ioele therefore does not identically describe nor in fact suggest that the event logs are separate counter logs for each provisioned customer or a global counter log that accounts for all traffic seen on the link. Moreover, the event logs taught by Ioele are not statistical counters that collect statistical information on network packets, but instead are conventional NT logs of events such as software, hardware, network and security problems. They are not counters logs of statistical information on packets.

Claims 13, 16

For the purposes of this appeal only, claims 13 and 16 stand or fall together. Claim 13 is representative of this group of claims.

Claim 13 serves to further distinguish the arrangement of claim 12 by requiring that the gateway maintains a global packet log for all traffic. Ioele does not describe the global packet log. The logs that Ioele does describe are event logs, convention logs of events such as software, hardware, network and security problems. The event logs are not global packet logs. Appellant discusses global packet logs in the specification at page 12, line 12 if the Board desires further information.

Claims 14 and 15

For the purposes of this appeal only, claims 14 and 15 stand or fall together. Claim 14 is representative of this group of claims.

Claim 14 limits claim 13 to require that the global packet log include a sample of all traffic seen on the link to which the gateway is connected. Ioele does not describe that the event logs result from a sample of all traffic seen on a link that is monitored. Claim 14 requires that the gateway performs the function of the base claim and claim 14.

Ioele in contrast, while clearly not describing the claimed global packet log also does not describe that the "operations and event log management system 140" actually performs any of

the functions or has the connections required by claim 14. That is, the "operations and event log management system 140" neither provides the global packet log nor monitors the link.

In contrast, Ioele discloses that the "operations and event log management system 140" uses a TEC engine. Specifically Ioele discloses that: "The Tivoli TEC engine is run on its own server and is used to roll up and monitor all event logs in the Internet hosting site. This allows the NSA of the Internet hosting site to catch any security issue or other areas of concern that may arise. Tivoli ensures the continuity of event log data by constantly monitoring the size of all NT event logs."

Presumably in the above passage, NT refers to Microsoft's NT operating system. However, the disclosed NT event logs are not global packet logs.

Claim 17

Claim 17 further limits claim 12, and requires that the gateway is a clustered gateway and includes a plurality of probes and a cluster head, with the cluster head having a process to aggregate traffic from the probes and to produce separate counter logs for each provisioned customer; and a global counter log, and produce detection heuristics.

The examiner contends that Ioele teaches this feature at Figure 1, Col. 6, lines 31-61. Ioele possess no teachings that would suggest much less describe a clustered gateway, a plurality of probes and a cluster head … .

At the cited passage of Ioele, the reference merely discusses two Intrusion Detection Systems and Firewalls, none of them however are disclosed as clustered and including a plurality of probes and a cluster head … as required by claim 17.

Claims 18- 22

For the purposes of this appeal only, claims 18-22 stand or fall together. Claim 18 is representative of this group of claims.

Claim 18 further limits claim 11, requiring that the provisioned monitor includes a virtual monitor for the physical link on which the provisioned monitor is deployed and is configured to be an independent node in the network capable of issuing attack warnings and responses to

attack queries independently from other virtual monitors of the provisioned monitor. Ioele discloses no such arrangement.

Claims 23

Claim 23 further limits the arrangement of claim 22 to require that the control center is adapted to distinguish an attack on a single provisioned customer associated with a virtual monitor and an attack on the link(s) on which the monitor is physically deployed.

Claims 24, 25, 27 and 28

For the purposes of this appeal only, claims 24, 25, 27 and 28stand or fall together. There is no claim 26. Claim 24 is representative of this group of claims.

Claim 24 distinguishes over Ioele since the reference fails to describe that ... collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs and maintaining separate counter logs for each provisioned customer, and a global counter log that accounts for all traffic seen on the links on which collecting occurs.

The examiner used the same basis to reject claim 24 as was used to reject claim 11. The examiner contends with respect to these later features that Ioele teaches: "... the provisioned monitor maintaining separate counter logs for each provisioned customer (Ioele, column 6 lines 45-46) and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to (Ioele, column 7 lines 37-64)."

Ioele does not specifically suggest, much less describe collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs and maintaining separate counter logs for each provisioned customer, and a global counter log that accounts for all traffic seen on the links on which collecting occurs. Ioele, at Col. 7 lines 37-64 (quoted above in the discussion of claim 11) does not identically describe nor suggest these features nor "a global counter log that accounts for all traffic seen on the links on which collecting occurs." The event logs are not counter logs nor are the separate counter logs for each provisioned customer nor are the event logs a global counter log that accounts for all traffic seen on the links. Moreover, the event logs taught by Ioele are not

statistical counters that collect statistical information on network packets, but instead are convention logs of events such as software, hardware, network and security problems.

Claim 29

Claim 29 is directed to a method of thwarting attacks on a victim data center ... and includes collecting statistical information for a plurality of links that are downstream from links on which collecting occurs, performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic and communicating alerts that arise from the traffic analysis.

Claim 29 distinguishes over Ioele since the reference fails to describe the feature of collecting as discussed in claims 11 and 24 and in addition, fails to describe performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic. Ioele does not process statistical information to perform analysis to identify malicious traffic. Rather, Ioele uses an IDS system that looks for attack signatures.

Claims 30-34

Each of claims 30-34 add distinct features to distinguish claim 29 over Ioele.

For example, Ioele does not describe whether at Col. 4, lines 7-20 or elsewhere that performing analysis occurs on statistical information collected for an individual one of the downstream links to identify malicious traffic intended for the individual one of the downstream links, as in claim 30. Ioele does not describe that analysis occurs on statistical information nor does Ioele describe that analysis is performed on traffic intended for an individual one of downstream links. Rather, Ioele discusses back tracing of addresses from which attacks originated from. That however deals with tracing the source of a DOS attack. Claim 30 in contrast claims to use addresses to maintain provisioned DOS monitoring on a per customer basis.

Claim 31, requiring that communicating to a control center occurs on a downstream link basis, is not disclosed in Ioele. Rather, the operations and event log management system 140 does not feature this element.

Similarly claim 32, which requires that communicating occurs on a downstream link basis to a control center that determines a response to the attack or claim 33... communicating occurs on a downstream link basis over a dedicated, hardened network to a control center that determines a response to the attack are not suggested by Ioele for reasons discussed above.

Claim 34 directed to filtering the identified malicious traffic and to eliminate the malicious traffic from reaching the one of the downstream links is allowable over Ioele for analogous reasons generally discussed in claim 4.

Conclusion

Appellant submits, therefore, that Claims 1-25 and 27-34 are allowable over the cited art. Therefore, the Examiner erred in rejecting Appellant's claims and should be reversed.

Respectfully submitted,

Date: 4/2/03

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

Appendix of Claims

1. A monitoring device disposed for thwarting denial of service attacks on a data center, the monitoring device comprising:

a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links and collect statistical information on packets that are sent between the network and the data center over the coupled physical links for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

2. The monitoring device of claim 1 wherein the monitoring device is coupled to a control center through a dedicated, private network.

3. The monitoring device of claim 2 wherein the device further comprises:

a communication process that communicates the statistical information on packets with the control center, and which receives queries or instructions from the control center.

4. The monitoring device of claim 1 wherein the monitoring device is a gateway device and further comprises:

a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

5. The monitoring device of claim 1 wherein the monitoring device is a data collector device.

6. The monitoring device of claim 4 wherein the gateway comprises:

a process to aggregate traffic from the various links and to produce logs and detection heuristics.

7. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on; and

communicating data, over a dedicated network, to a control center.

8. The monitoring device of claim 7 wherein the device is a gateway device, which further comprises:

installing filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

9. The monitoring device of claim 7 wherein the monitoring device is a data collector device.

10. The monitoring device of claim 7 wherein collecting occurs for inbound and/or outbound traffic.

11. An arrangement disposed to monitor a link between a data center and a network for thwarting denial of service attacks on the data center, the arrangement comprising:

a provisioned monitor, placed on selected links in the data center so that the provisioned monitor examines traffic entering or leaving that data center on the selected links and collects statistical information for a plurality of provisioned customers, which are on links that are downstream from the selected links that the provisioned monitor is disposed on, the provisioned monitor maintaining separate counter logs for each provisioned customer; and

a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.

12. The arrangement of claim 11 wherein the provisioned monitor is a gateway that maintains separate packet logs for each monitor.

13. The arrangement of claim 12 wherein the gateway maintains a global packet log for all traffic.

14. The arrangement of claim 13 wherein the global packet log includes a sample of all traffic seen on the link to which the gateway is connected.

15. The arrangement of claim 14 wherein packet analysis for a particular monitor happens by classifying packets based on addresses at the time of the analysis.

16. The arrangement of claim 13 wherein the gateway maintains duplicate packets, keeping both a global packet log and a packet log for each virtual monitor.

17. The arrangement of claim 12 wherein the gateway is a clustered gateway and includes a plurality of probes and a cluster head, with the cluster head having a process to aggregate traffic from the probes and to produce separate counter logs for each provisioned customer; and a global counter log, and produce detection heuristics.

18. The arrangement of claim 11 wherein the provisioned monitor including a virtual monitor for the physical link on which the provisioned monitor is deployed is configured to be an independent node in the network capable of issuing attack warnings and responses to attack queries independently from other virtual monitors of the provisioned monitor.

19. The arrangement of claim 18 wherein the provisioned monitor including all of the provisioned monitor's virtual monitors act as one node in the distributed network.

20. The arrangement of claim 19 wherein the provisioned monitor acts as an intermediary between virtual monitors and the rest of the network and includes a process to maintain communications with the control center and to reply to attack queries.

21. The arrangement of claim 18 wherein the provisioned monitor's virtual monitors have filters installed on a per virtual monitor basis.

22. The arrangement of claim 18 wherein when a virtual monitor detects an attack on a provisioned customer, information is conveyed both to the control center and to a hosting provider's management interface.

23. The arrangement of claim 22 wherein the control center is adapted to distinguish an attack on a single provisioned customer associated with a virtual monitor and an attack on the link(s) on which the monitor is physically deployed.

24. A method of thwarting attacks on a victim data center coupled to a network comprises:

collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs; and

maintaining separate counter logs for each provisioned customer; and a global counter log that accounts for all traffic seen on the links on which collecting occurs.

25. The method of claim 24 wherein collecting occurs on a gateway that passes network packets, the gateway being disposed at an edge of the network.

27. The method of claim 24 wherein collecting occurs on a data collector that samples network packets, the data collector being disposed at a location that is at a large aggregation link in the network for the data center.

28. The method of claim 24 further comprising:

performing, by the provisioned gateway, intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

29. A method of thwarting attacks on a victim data center coupled to a network comprises:

collecting statistical information for a plurality of links that are downstream from links on which collecting occurs;

performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic; and

communicating alerts that arise from the traffic analysis.

30. The method of claim 28 wherein performing analysis occurs on statistical information collected for an individual one of the downstream links to identify malicious traffic intended for the individual one of the downstream links.

31. The method of claim 28 wherein communicating to a control center occurs on a downstream link basis.

32. The method of claim 28 wherein communicating occurs on a downstream link basis to a control center that determines a response to the attack.

33. The method of claim 28 wherein communicating occurs on a downstream link basis over a dedicated, hardened network to a control center that determines a response to the attack.

34. The method of claim 28 further comprising:

filtering the identified malicious traffic and to eliminate the malicious traffic from reaching the one of the downstream links.

Evidence Appendix

None

Related Proceedings Appendix

None